Volume 104 | Issue 2 Article 5

January 2002

Wired, Wonderful West Virginia - Electronic Signatures in the Mountain State

Robin C. Capehart
Steptoe and Johnson

Mark A. Starcher
Scanmark Limited

"WIRED, WONDERFUL WEST VIRGINIA"[1] – ELECTRONIC SIGNATURES IN THE MOUNTAIN STATE

Robin C. Capehart[*]
Mark A. Starcher[**]

[1] Thanks to the West Virginia Governor's Office of Technology, which coined this phrase in publicizing a May 2001 conference highlighting technology accomplishments in state government.

[*] Of Counsel - Steptoe and Johnson; Associate Professor, Marshall University; former Secretary of Tax and Revenue for the State of West Virginia; B.A., J.D., West Virginia University; LL.M. in Taxation, Georgetown University.

[**] President, Scanmark Limited, McLean VA. B.S., J.D., West Virginia University, M.S., The Johns Hopkins University, LL.M, Georgetown University. The author provides computer consulting and database management services to clients, including the State of West Virginia.

I. INTRODUCTION: THE DIGITAL AGE IN WEST VIRGINIA

The so-called "digital age" has changed the way West Virginians work, play, and interact. Many businesses, government agencies, and citizens within the state use some form of "information processing system"[2] to interact, conduct business, and transfer information. However, throughout most of the state's history, common transactions such as the sale of property subject to the Statute of Frauds[3] or the filing of a corporate state tax return[4] in West Virginia could not

---

[2] The West Virginia Code defines the term "information processing system" as an "electronic system for creating, generating, sending, receiving, storing, displaying or processing information." W. VA. CODE § 39A-1-2(11) (Supp. 2001).

[3] West Virginia Code section 46-2-201(1) provides:

> Except as otherwise provided in this section a contract for the sale of goods for the price of $500 or more is not enforceable by way of action or defense unless there is some *writing* sufficient to indicate that a contract for sale has been made between the parties and *signed* by the party against whom enforcement is sought or by his authorized agent or broker. A *writing* is not insufficient because it omits or incorrectly states a term agreed upon but the contract is not enforceable under this paragraph beyond the quantity of goods shown in such writing.

W. VA. CODE § 46-2-201(1) (2001) (emphasis added).

[4] West Virginia Code section 11-13A-15 provides, in part, as follows:

> (b) Signing of corporation returns. – The return of a corporation shall be *signed* by the president, vice president, treasurer, assistant treasurer, chief accounting officer or any other officer duly authorized so to act. In

be completed in electronic form. Each of the aforementioned acts required citizens to satisfy legal requirements rooted in a paper-based world where physical attributes (*i.e.*, handwritten signatures and the paper itself) authenticated and documented transactions between unrelated persons. However, under the West Virginia Uniform Electronic Transactions Act ("WVUETA"), these transactions may be accomplished in electronic form through the use of "electronic signatures;"[5] the digital analogy to the signature requirement for paper documents.[6]

The electronic signature legislation represents one of several legislative efforts in the past several years to

> promote electronic commerce and online government by clarifying the legal status of electronic records and electronic signatures in the context of writing and signing requirements imposed by law; to permit and encourage the continued expansion of electronic commerce and online government through the operation of free market forces rather than proscriptive legislation; to promote public confidence in the validity, integrity and reliability of electronic commerce and online government; and to promote the development of the legal and business infrastruc-

---

> the case of a return made for a corporation by a fiduciary, such fiduciary shall *sign* the return. The fact that an individual's name is *signed* on the return shall be prima facie evidence that such individual is authorized to *sign* the return on behalf of the corporation. . . .
>
> (d) *Signature* presumed authentic. – The fact that an individual's *name is signed to a return*, statement, or other document shall be prima facie evidence for all purposes that the return, statement or other document was actually *signed* by him. . . .

W. VA. CODE § 11-13A-15 (1999) (emphasis added).

[5] Also known as "digital signatures." Throughout this Article, both terms are used interchangeably.

[6] West Virginia Code section 2-2-10(c) provides that for purposes of statutory construction,

> The words "written" or "in writing" include any representation of words, letters or figures, whether by printing, engraving, writing or otherwise. But when the signature of any person is required, it must be in his or her own proper handwriting, or his or her mark, attested, proved or acknowledged: *Provided, That unless a provision of this code specifically provides otherwise, an electronic signature satisfies this signature requirement if the electronic signature meets the requirements of subsection (a), section three, article five, chapter thirty nine of this code* . . . .

W. VA. CODE § 2-2-10(c) (1999) (emphasis added). The emphasized language was added by former West Virginia Code section 39-3-5, which was repealed by the WVUETA. *See* W. VA. CODE § 39-3-5, *repealed by*, S.B. 204, enrolled April 14, 2001. Presumably, this section should now be interpreted to reference the provisions of § 39A-1-7(d), describing the legal recognition of electronic signatures in any law requiring a signature. W. VA. CODE § 39A-1-7(d) (Supp. 2001).

> ture necessary to support and encourage electronic commerce and online government.[7]

Prior to the WVUETA, additional technological measures put in place in West Virginia include the formation of an oversight office within the Governor's office to set and promote technology standards within state agencies;[8] the passage of the Electronic Signatures Authorization Act ("ESAA") in 1998,[9] the precursor to the WVUETA; and the passage of the Medical Practices Act in 1999,[10] which permitted persons regulated under its provisions to use electronic signatures in the course of medical practice. The WVUETA represents a major step forward, but work remains to create a digital infrastructure that supports the digital delivery, authentication, and storage of business and government infor-

---

7 *See* W. VA. CODE § 39-5-1, *repealed by* S.B. 204, enrolled April 14, 2001.

8 In 1997, the West Virginia Governor's Office of Technology was created pursuant to West Virginia Code section 5-1B-3. Section 5-1B-4(a) provides, in part, that "with respect to all state spending units the chief technology officer shall

> (3)Evaluate, in conjunction with the information services and communications division of the department of administration, the economic justification, system design and suitability of information equipment and related services, and review and make recommendations on the purchase, lease or acquisition of information equipment and contracts for related services by the state spending units; . . .
>
> . . . .
>
> . . . (6) Create new technologies to be used in government, convene conferences and develop incentive packages to encourage the utilization of technology.

W. VA. CODE § 5-1B-4(a) (1999). With respect to executive agencies within the state, West Virginia Code section 5-1B-4(b) provides far broader powers and permits the chief technology officer to

> (1) Develop a unified and integrated structure for information systems for allexecutive agencies;
>
> (2) Establish, based on need and opportunity, priorities and time lines for addressing the information technology requirements of the various executive agencies of state government; . . . .W. VA. CODE § 5-1B-4(b) (1999).

9 W. VA. CODE §§ 39-5-1 to -8, *repealed by* S.B. 204, enrolled April 14, 2001.

10 W. VA. CODE section 30-3-13 states,

> Persons covered under this article may be permitted to utilize electronic signature or unique electronic identification to effectively sign materials, transmitted by computer or other electronic means, upon which signature is required for the purpose of authorized medical practice. Such signatures are deemed legal and valid for purposes related to the provision of medical services.

W. VA. CODE § 30-3-13 (Supp. 2001).

mation in the Mountain State.[11]

This Article considers the significance of digital signatures, from both legal and technological viewpoints; provides a brief introduction to "public key" infrastructure, the principal technology underlying electronic and digital signatures;[12] and reviews legislative developments in the digital signature area in West Virginia. The Article also reviews some of the business and auditing issues surrounding the adoption of the public key infrastructure. The Article concludes with suggestions for additional measures that are needed in order to fully leverage the technological infrastructure for use in business and government transactions.

II. WHY DIGITAL SIGNATURES?

A. *Contracts Law Perspective*

The advantages afforded by digital technology allow contractual obligations to be completed rapidly over great distances with no requirement that parties ever meet or exchange tangible forms of an agreement. However, although these digital characteristics offer significant time advantages to the parties, without a digital signature they can cause problems because they tend to run counter to long-standing legal formalities that are intended to address disputes of offer and acceptance as well as interpretation of contracts.[13] With the introduction of digital signatures, those problems can be alleviated.

For instance, consider several particular functions that are served by the signature formality in contract law: the evidentiary function, the channeling function, and the cautionary function.[14] The evidentiary function is a means by which a record can be accessed that may serve to interpret the dealings of the parties.[15] Traditionally, this function is satisfied by the tangible paper records associated with a contract. The digital age creates several problems with this function. First, the communications between parties are in an intangible form,

---

[11] For example, the WVUETA specifically excludes certain transactions from its application including laws "governing the creation and execution of wills, codicils or testamentary trusts." W. VA. CODE § 39A-1-3(b)(1) (Supp. 2001).

[12] The terms "digital signature" and "electronic signature" are defined in sections 39A-3-1(3) and 39A-1-2(8) of the West Virginia Code, respectively. For purposes of this Article, a digital signature is a type of electronic signature.

[13] Henry Perritt has written an excellent general discussion of this topic. *See generally* HENRY H. PERRITT, LAW AND THE INFORMATION SUPERHIGHWAY § 9.06 (2d ed. 2001).

[14] *See id.* § 9.06, at 581 (citing Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 123-24 (1989) (referencing Lon Fuller, *Consideration and Form*, 41 COLUM. L. REV. 799 (1941))). *See also* Swerhun v. General Motors Corp., 812 F. Supp. 1218, 1222 (M.D. Fla. 1993) (citing these elements as the basis for enforcing promissory estoppel theory).

[15] *See* PERRITT, *supra* note 13 (citing Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 123-24 (1989)).

and, second, the communications themselves are inherently malleable.[16] However, the use of digital signatures can act to authenticate valid forms of communication and can also validate document versions.

The channeling function is also difficult to accomplish *via* electronic means.[17] This function is best described through the application of the "four corners" principle of contract law, in which the intent and purpose of the parties can be ascertained through a single document, or significantly limited in scope through use of integration clauses and the parole evidence rule.[18] This function is difficult to achieve in an age where electronic documents can be created and transported instantly. Contracting in the digital age typically consists of a collection of electronic documents, including, for example, email (including electronic receipts); successive document drafts with suggested revisions, deletions, and comments; electronic images; and digital audio and video files.[19] Hence, one is left to sift through the dross of electronic communication to determine which items truly reflect the intent of the parties.[20] Again, the use of digital signatures allows contracting parties to indicate the relative weight of individual documents by attaching digital signatures only to those of legal significance.[21]

The cautionary function, although difficult to implement in a digital format, can be achieved through security measures that are intended to restrict access by affected parties to documents or transactions that could be construed as contracts.[22] A simple example of this type of function is the acceptance screen for terms and conditions in a typical shrink-wrapped software license. The end-user is typically presented with an electronic license agreement that provides terms and conditions, which the user may "scroll" through to read. To complete the software installation, the end-user must click a box, indicating that he or she accepts the terms of the license. If the user chooses not to accept the license, the installation process is aborted. Although one could argue over the contractual validity of this type of unilateral presentation, it does illustrate a means by which protective or cautionary functions are served in the digital age.[23]

---

16 *See id.* § 9.06, at 581-82.

17 *See id.*

18 *See id.*

19 *See id.*

20 *See id.*

21 In effect, the digital signature acts as an integration clause that limits the scope of contract interpretation to those documents that have been digitally signed. *See id.* § 9.06, at 583.

22 *See id.*

23 *See* PERRITT, *supra* note 13, § 9.07, at 588-93.

B. *Technology Perspective*

The means by which digital documents are transmitted over publicly shared media, the "malleability" of electronic documents, and the lack of a time element as a means of authentication create a separate and distinct rationale for digital signatures. In this case, the digital signatures are used to validate the processes incidental to communications over public networks.[24] First, the signature authenticates the identity and authority of individuals and corporations communicating electronically.[25] Second, it is required to assure the integrity of the electronic communication and to detect any unauthorized modifications or communication interception that could result in modifications to that message in transit.[26] Third, the digital signature protects messages and records against interception, unauthorized access, and disclosure of sensitive or confidential information.[27] Finally, it can be used to control access to authorized parties only.[28]

III. PUBLIC KEY INFRASTRUCTURE ("PKI") – A PRIMER

The technology that supports the digital signature concept is rooted in cryptography, a branch of applied mathematics concerned with information security.[29] Simply put, a cryptograph is a mathematical function that can be applied to information to create a non-obvious result.[30]

A. *Encryption Basics*

A very simple example illustrates the concept. Assume that the letters of the alphabet are numbered consecutively from 1 (A) to 26 (Z). The word "dog" (referred to as "plaintext") under this scenario can be digitally represented by the string "042007," two digit codes that show the sequential order of the letters

---

[24] In many ways, this function is analogous to the "seal" requirements imposed under common law. The seal acted to authenticate the author of the document and also served as a means to determine whether the message had been intercepted or modified in transit. *See* W. VA. CODE §§ 46-2-203, -2A-203 (2001) (seals are inoperative for purposes of defining a "sealed instrument").

[25] *See* PKI ASSESSMENT GUIDELINES, V 0.30 (Public Draft for Comment No. 25, 2001), *available at* http://www.abanet.org/scitech/ec/isc/pagv30.pdf (last visited Jan. 29, 2002) (hereinafter PAG) (on file with *The West Virginia Law Review*).

[26] *See id.*

[27] *See id.*

[28] *See id.* These guidelines are a sequel to the 1996 Digital Signature Guidelines released by the same committee. *See* DIGITAL SIGNATURE GUIDELINES, *available at* http://www.abanet.org/scitech/ec/isc/dsg.pdf (last visited Jan. 29, 2002) (hereinafter DSG) (on file with *The West Virginia Law Review*).

[29] *See* PAG, *supra* note 25, at 301.

[30] *See id.*

that spell "dog." Although coded, the information is easily deciphered. One way to make the code less obvious is to apply a mathematical function to the numerical code that represents "dog." For example, one could multiply the derived code by the number 3 to arrive at a new value. Hence, the numerical string "126021" would represent the word "dog." That result could be sent to another person, and, assuming that the other person had the key (*i.e.*, the mathematical function used to derive the string), he or she could "decrypt" the message (*i.e.*, derive the plaintext message) by dividing each two-digit pair within the string by three, and referencing the sequential number of the alphabet to determine the message. Another way to encrypt the same message is to use an offset to scramble the letters of the alphabet. Using an offset of one to modify the original scenario, presented above, the word "dog" is represented by the string "031906."[31]

Modern encryption is based on these same principles. In real world scenarios, however, the techniques described above are combined to create cryptographs that are much more difficult to decipher. Unlike the scenario sketched out above in which a string was multiplied by three to create a code, modern encryption uses mathematical functions based on prime numbers that are over one hundred (100) digits in length. These mathematical functions are referred to as "hash values" and form the basis for the encryption keys that are used in most programs today.[32] This mathematical function can then be combined with an offset key to further complicate the coding.[33]

B. Symmetric Key Cryptology

The example given above requires that each person involved in the message process have access to the same key to encrypt and decrypt the message. In this case, a single key is used to encrypt and decrypt the message. Unless the receiver knows that each of the numbers in the first example was multiplied by three, it will take longer to decrypt the message. This is referred to as "symmetric key cryptology."[34]

Although very secure and efficient, symmetric key cryptology has two drawbacks that prevent it from being used in a public infrastructure. First, two

---

[31] In this case, the offset results in the letter "B" being coded as 01, "C" as 02, and so forth, with the letter "A" being coded as 26. The offset system was originally used by Julius Caesar and the method is still referred to as a "Caesar Cipher."

[32] *See* DSG, *supra* note 28, at 9-11.

[33] The terms "40-bit encryption" and "128-bit encryption," commonly used in commercial electronic transactions, refer to the length of the key used to encode a message. To illustrate the dimensions of these two encryption systems, 128-bit encryption is 309,485,009,821,345,068,724,781,056 times "stronger" than 40-bit encryption. *See What is the Difference Between 128-bit and 40-bit Encryption?*, Netscape, *at* http://help.netscape.com/kb/consumer/19971208-6.html (last updated June 13, 2001) (on file with *The West Virginia Law Review*).

[34] For a tutorial on encryption techniques used in PKI, see PAG, *supra* note 25, at 301.

users interacting for the first time over a public network have no way of securely transmitting symmetrical keys to be used in subsequent transmissions. Second, the transfer of any key in this situation is subject to the possibility of interception or modification by a third party.[35]

C. *Asymmetric Key Cryptology*

To deal with the perceived shortcomings of symmetric key cryptology, a different type of cryptograph was created that uses two related keys to produce a digital signature. In asymmetric key cryptology, the first key, held by the party that will be receiving the message, is referred to as the "private key" and is uniquely known to the recipient.[36] The second key, a mathematical derivate of the private key[37] is referred to as the "public key," which can be distributed to parties that may potentially interact with the recipient.[38] To encrypt a message, the sender must retain the public key of the recipient and the message will be encrypted using this key.[39] The recipient, upon receipt, will then use their "private key" to decrypt the message back to plaintext format so that it may be viewed.[40] This "hand-in-glove" technique (*i.e.*, the matching of the public and private key) allows only the intended recipient to view the plaintext version of the message.[41] This type of cipher is referred to as "asymmetric key cryptology."[42]

The asymmetric key also holds another feature that not only validates the user who created the message, but also assures that the message was not intercepted or modified in transit. This feature is referred to as a "hash function," which is essentially a digital fingerprint of the message, as transmitted from the user. By comparing the hash value received with that represented by the message itself, this function allows the end-user to determine whether the message has been intercepted or tampered with during transit.[43] This process is analogous to a letter that arrives *via* registered mail.

---

35 *Id.*

36 *See* PAG, *supra* note 25, at 305.

37 *See generally supra* note 34. Potentially, the derivative mathematical function used to create the public/private key combination can have keys that number 2^{1024} power. For a discussion of the possible key values associated with 128-bit encryption, see *supra* note 34 and accompanying text.

38 *See* DSG, *supra* note 28, at 9.

39 *See* PAG, *supra* note 25, at 305.

40 *See id.*

41 *See id.*

42 *See* PAG, *supra* note 25, at 301.

43 DSG, *supra* note 28, at 9.

D. *Digital Signatures*

Digital signatures are derivates of public key cryptology.[44] The "signer" of an electronic document creates a unique hash function based on the message to be transmitted and the private key that is in his or her possession. Typically, this digital signature (hash function) is then attached to the "signed" message (or sent with linkage to the transmitted message).[45] Digital signature verification is accomplished when the receiving party, using an identical hash function, computes a new hash result with the public key and checks this value against the hash function that was transmitted or referenced in the delivered message.[46] This verification will assure that the digital signature was created using the corresponding private key, and that the message was not altered in transit (in which case the computed hash functions would not match).[47]

E. *Digital Certificates*

An integral part of the digital signature process is the ability to freely distribute public keys to third parties for use in message verification. Distribution of the public key, however, requires that a receiving party obtain that key from an institution with assurances that (1) the public key is associated with the person that it references, and (2) that the person referenced is actually the person who created the message.[48] This function is handled through the use of digital certificates.

Digital certificates are messages indicating that a public key belongs to a particular person or organization. Certificates are issued by organizations known as certificate authorities ("CAs") and are, themselves, digital signatures

---

[44] PAG, *supra* note 25, at 301.

[45] DSG, *supra* note 28, at 9; PAG, *supra* note 25, at 301-03.

[46] DSG, *supra* note 28, at 9; PAG, *supra* note 25, at 301-03.

[47] As previously mentioned, this verification also satisfies several contract law principles, including signer verification; message authentication, which is an affirmative act on the part of the signer (i.e., the signer must affirmatively identify the message to be signed and commence the signature process); and efficiency (the verification process can be handled automatically with no human intervention, unlike manual validation using signature cards). *See* PAG, *supra* note 25, at 303.

[48] Identity theft can also occur through the carelessness of individuals who have digital signatures. Typically, digital signature programs require the end-user to enter a series of letters, numbers, and symbols, which are then converted into a unique mathematical function that is used in the encoding of messages. This unique set (sometimes exceeding 30 characters in length) is typically saved by the end-user and archived for future reference. The actual digital signature (the hash function) can be called for a user's desktop computer using a user-name and password combination. Identity theft is possible in situations in which the user-name/password combination or the original alphanumeric key is compromised. *See* PAG, *supra* note 25, at 301-09.

(with the certificate authority using its private key to validate the message).[49] Certificate authorities, in turn, can be validated by higher CAs, essentially creating a "certificate chain."[50] Ultimately, the user reaches the "root certificate," *i.e.*, one in which the certificate authority self-authenticates for purposes of determining the validity of the certificates.[51]

The West Virginia Uniform Electronic Transactions Act ("WVUETA")[52] uses the public key infrastructure/digital signature technique to accomplish authentication and validation. However, before delving into the specifics of the WVUETA, we will review its legislative antecedents to show the development of the "digital age" in West Virginia, which will give added insight into the purposes of the WVUETA.

IV. SIGNATURE LEGISLATION PRIOR TO THE WEST VIRGINIA UNIFORM ELECTRONIC TRANSACTIONS ACT

Prior to the 2001 Legislative session, the West Virginia Legislature had several occasions to address the signature requirements that were set forth in various code sections. These actions gradually led the state away from the individual signature requirements under early contract and common law and laid the foundation for the WVUETA.

A. Uniform Facsimile Signatures of Public Officials Act ("UFSPOA")

The "signature" requirements for business transactions are by no means limited to the digital age. Indeed, the Legislature has had occasion to review the statutory schemes and adapt them accordingly, as state law in West Virginia is replete with requirements that public officials affix their "signatures" to a variety of public documents. For example, the thousands of paychecks that the state distributes to its employees are required by law to contain the signatures of the state auditor and treasurer.[53] Clearly, the days have long passed since it has been physically possible to comply with this requirement with a handwritten signature.

In 1965, the Legislature addressed this problem by enacting the Uniform Facsimile Signatures of Public Officials Act ("UFSPOA").[54] In essence,

---

49 *See id.*

50 *See id.*

51 Root certificates are subject to detailed security provisions that prevent, for example, the transport of that type of certificate across a public network. *See* PAG, *supra* note 25, at 305.

52 W. VA. CODE §§ 39A-1-1 to -3-4 (Supp. 2001).

53 West Virginia Code section 12-4-4 requires that the signatures of the Treasurer and Auditor be affixed to all checks and warrants issued by their respective offices. W. VA. CODE § 12-4-4 (2000).

54 W. VA. CODE §§ 6-14-1 to -8 (2000).

the UFSPOA was West Virginia's first divergence from the traditional requirement of a separate, individually written signature. The purpose of this provision was to permit certain public officials to use or cause to be used a facsimile signature in lieu of his or her handwritten signature on specified public documents. With this statutory authority, such public officials could avoid the potential Herculean task of signing a great number of instruments required by law.

Under the UFSPOA, "authorized officers" include state, county, municipal officials, including members of boards or commissions whose signatures were required or permitted on a public security or instrument of payment.[55] The UFSPOA describes the "facsimile signature" of a public official as "a reproduction by engraving, imprinting, stamping or other means of the manual signature of an authorized officer."[56] To use a facsimile signature, the statute requires the public official to file with the Secretary of State his manual signature certified by him under oath.[57]

At the time of enactment, a manual signature was a practical way to execute a public security or instrument of payment. However, times changed and reliance upon manual signatures became impractical. Through its enactment of the UFSPOA in 1965, the West Virginia Legislature recognized, for the first time, that it would be necessary to adopt processes and procedures that were not contemplated when the operative statutes were enacted.

B. Electronic Signatures Authorization Act ("ESAA")

1. Purpose

The explosion in electronic commerce during the 1990's accelerated the need for statutory changes to reflect the evolution of the methods used by parties that were engaging in commercial, personal, and governmental transactions. In 1998, the West Virginia Legislature took its first step by enacting the Electronic Signatures Authorization Act ("ESAA"). It is important to note that the ESAA is no longer in effect in West Virginia as it was repealed by the WVUETA. Its development and content, however, are crucial to the understanding of the WVUETA because when the WVUETA was enacted, several of the provisions of the ESAA were reenacted in some form in the WVUETA.

---

55 W. VA. CODE § 6-14-1(c) (2000). West Virginia Code section 6-14-1(a) defines a "public security" as a "bond, note, certificate of indebtedness or other obligation for the payment of money issued by this state or by any of its departments, agencies, boards, commission or other instrumentalities or by any of its public corporations, political subdivisions, municipal corporations or other governmental units." W. VA. CODE § 6-14-1(a) (2000). West Virginia Code section 6-14-1(b) further defines "instrument of payment" as "a check, draft, warrant or order for the payment, delivery or transfer of funds." W. VA. CODE § 6-14-1(b) (2000).

56 W. VA. CODE § 6-14-1(d) (2000).

57 W. VA. CODE § 6-14-2 (2000).

The purpose of the ESAA was fourfold:

(1) To clarify "the legal status of electronic records and electronic signatures in the context of writing and signing requirements imposed by law";[58]

(2) "[T]o establish standards and processes to facilitate the use of electronic signatures in all governmental transactions by state agencies";[59]

(3) To authorize government agencies to accept "electronic signatures in lieu of original signatures";[60] and

(4) To validate electronic signatures in transactions in which the signing party signs by electronic signature in good faith and the receiving party agrees to accept the electronic signature.[61]

2. Electronic Signatures

The ESAA defined an electronic signature as "any identifier or authentication technique attached to or logically associated with an electronic record that is intended by the person using it to have the same force and effect as a manual signature."[62] This broad definition set forth three requirements for an electronic signature. First, an electronic signature had to be an "identifier or authentication technique."[63] We may conclude from this open-ended requirement that the ESAA did not require the parties to use an electronic signature that involves a specific type of technology. Second, the electronic signature had to be "attached to or logically associated with an electronic record."[64] Once again, the ESAA did not require a specific type of technological attachment or association with the electronic record. Instead, the provision required only that the electronic signature be attached or associated in some reasonable manner. Third, the signer had to intend for the electronic signature to operate as if he has signed the message manually.[65] At this point, the ESAA fell short of providing any guidance regarding assertions of misuse of an electronic signature. We may assume that the appearance of the electronic signature would establish the presumption

---

58 W. VA. CODE § 39-5-1, *repealed by* S.B. 204, enrolled April 14, 2001.

59 W. VA. CODE § 39-5-4(a), *repealed by* S.B. 204, enrolled April 14, 2001.

60 W. VA. CODE § 39-5-5(a), *repealed by* S.B. 204, enrolled April 14, 2001.

61 W. VA. CODE § 39-5-6(a), *repealed by* S.B. 204, enrolled April 14, 2001.

62 W. VA. CODE § 39-5-2(e), *repealed by* S.B. 204, enrolled April 14, 2001.

63 *Id.*

64 *Id.*

65 *Id.*

that the signer intended its use absent any type of fraud or misrepresentation. It would only seem reasonable then that any attempt by the signer to disavow the legitimacy of his electronic signature would have required that he provide the proof necessary to show inappropriate use.

The ESAA described three types of electronic signatures: (1) a digitized signature; (2) a digital mark; and (3) a digital signature.[66] Under the ESAA, a "digitized signature" was created when a person entered his signature on a recording device that converts the signature to an image, which is attached to the electronic record.[67] In essence, a digitized signature under the ESAA was a form of a facsimile signature as described in the UFSPOA.[68] When used, the digitized signature verified or certified the electronic record in a form that appeared as if a manual signature had been used. [69]

In contrast, under the ESAA a "digital mark" was essentially a security device that restricted access to the electronic record to authorized individuals.[70] It consisted of an electronic code that is entered into the electronic record with an access protocol, such as a password, personal identification number ("PIN"), encrypted card, or some other type of device.[71] Once the proper code is given, approval or confirmation was given to enter the electronic record. A familiar type of digital mark is the PIN number given for access to a bank account through an automated teller machine ("ATM"). Access to a computer's operating system or specific type of software often requires a digital mark in the form of a user name and password.[72]

The ESAA included "digital signatures" as a third type of electronic signature.[73] A "digital signature" was defined as

> a message transformed using an asymmetric cryptosystem so that a person having the initial message and the signer's public key can accurately determine: (A) whether the transformed message was created using the private key that corresponds to

---

66 *Id.*

67 W. VA. CODE § 39-5-2(e)(1), *repealed by* S.B. 204, enrolled April 14, 2001.

68 West Virginia Code section 6-14-1(d) defines a "facsimile signature" as "a reproduction by engraving, imprinting, stamping or other means of the manual signature of an authorized officer." W. VA. CODE § 6-14-1(d) (2000).

69 The use of a "digitized signature" neither certifies nor verifies the message to which it is attached. As an image file, the digitized signature can be easily reproduced and attached to any number of documents. The Legislature, we presume, was attempting to extend the facsimile signature legislation to public officials for any type of electronic document. Thankfully, this definition was not retained in the 2001 legislation.

70 W. VA. CODE § 39-5-2, *repealed by* S.B. 204, enrolled April 14, 2001.

71 W. VA. CODE § 6-14-2(e)(2) (2000).

72 W. VA. CODE § 39-5-2, *repealed by* S.B. 204, enrolled April 14, 2001.

73 *Id.*

> the signer's public key; and (B) whether the initial message has been altered since the message was transformed.[74]

In short, under the ESAA, a "digital signature" referred to a process in which a mathematical formula secured and authenticated a message.[75]

A number of technological terms permeate this definition, such as "public key," "private key," and "asymmetric cryptosystem," and even the word "message" is a term of art. To the technologically enlightened, these terms may have common meanings. However, because the Legislature was creating laws that would also govern the technologically impaired, it would have been helpful for the Legislature to have further defined these terms.

It is interesting to note that although the definition included three types of "electronic signatures,"[76] the ESAA left the door open for the inclusion of future innovations by stating that electronic signatures included but *does not limit* the operation of this act to digitized signatures, digital marks and digital signatures.

3. Scope of the ESAA

While attempting to facilitate the use of electronic commerce, the Legislature, in adopting the ESAA, clearly did not intend to create substantive provisions that would require the use of electronic commerce or any specific type of technology in conducting electronic commerce. In fact, the legal effect of the ESAA was limited to circumstances in which:

a. the person or government agency receiving the message authorized its use;

b. the signer intended the digitized signature, digital mark or digital signature to be his signature; and

c. the receiving party did not know that the signer breached a duty or was not entitled to use the code or key which created the digital signature.[77]

Moreover, the ESAA did not: (1) preclude the use of electronic signatures under other substantive laws; (2) require a person to accept an electronic signature; or (3) prevent parties from establishing conditions or limitations re-

---

74 W. VA. CODE § 39-5-2(e)(3), *repealed by* S.B. 204, enrolled April 14, 2001.

75 Christopher B. Woods, Comment, *Commercial Law: Determining Repugnancy in an Electronic Age: Excluded Transactions Under Electronic Writing and Signature Legislation*, 52 OKLA. L. REV. 411, 415 (1999). Reference is made to this article for a more technological description of the digital signature process.

76 W. VA. CODE § 39-5-2(e), *repealed by* S.B. 204, enrolled April 14, 2001.

77 W. VA. CODE § 39-5-3(a), *repealed by* S.B. 204, enrolled April 14, 2001.

garding the use of electronic signatures.

Arguably, there appears to be an additional limitation. The definition sets forth three types of "electronic signatures": digitized signatures, digital marks, and digital signatures.[78] The provision also stated that the definition of electronic signature is not limited to those three types.[79] Yet, Section 3, the operative section of the ESAA, stated that electronic signatures would be accepted only if the signer intended to affix "[t]he original digitized signature, digital mark or digital signature . . ." to the message or a facsimile digitized signature was properly affixed by the signer's designee.[80] Thus, the requirements in the operative section of ESAA appeared to contradict the Legislature's intent as indicated by the definition and preclude the use of other forms of electronic signatures that presently exist or that may be created in the future.

4. Use of Electronic Signatures by State Agencies

The ESAA also attempted to encourage, promote, and support the an effective "online government" with the development of an electronic infrastructure.[81] The primary responsibility for creating such an infrastructure rested with the Secretary of State.

Section 4 of the ESAA instructed the Secretary of State and the State Auditor to promulgate regulations that establish standards and processes that will facilitate the use of electronic signatures in all governmental transactions involving state agencies.[82] This section also empowered the Secretary of State to:

a. serve as the certification authority and repository for state agencies;

b. regulate electronic transactions and digital signature verification;

c. contract with the federal government regarding the use of electronic transactions;

d. establish, by regulation, a system to issue public keys and other electronic transaction authentication devices; and

e. use private companies to provide the listed services.[83]

---

78 W. VA. CODE § 39-5-2(e), *repealed by* S.B. 204, enrolled April 14, 2001.

79 *Id.*

80 W. VA. CODE § 39-5-3(a)(2), *repealed by* S.B. 204, enrolled April 14, 2001.

81 W. VA. CODE § 39-5-1, *repealed by* S.B. 204, enrolled April 14, 2001.

82 W. VA. CODE § 39-5-4(a), *repealed by* S.B. 204, enrolled April 14, 2001. Section 64-9-2 of the West Virginia Code authorized the Secretary of State to issue legislative rules pertaining to the use of electronic signatures by state government agencies. W. VA. CODE § 64-9-2 (2000).

83 W. VA. CODE § 39-5-4, *repealed by* S.B. 204, enrolled April 14, 2001.

Despite the sweeping authority granted to the Secretary of State, section Four appeared to stop short of allowing the Secretary of State to require state agencies to use a particular technology. However, the Secretary of State could have offered, through regulation, alternative technologies to authorize electronic technologies.[84]

Under the ESAA, the power to decide whether a governmental entity would accept an electronic signature rested with each particular agency.[85] This included city and county governments, boards of education, and other types of local boards and commissions. Although state agencies were required to yield to the authority of the Secretary of State, other governmental entities could elect to utilize the Secretary of State's authority to verify and register digital signatures subject to public notice of the entity's intent to do so.[86]

As the registry for governmental digital signatures, the Secretary of State also retained the power to revoke any signature key if he or she determined that the digital signature key has been stolen, fraudulently used, or compromised.[87] By establishing the authority of the Secretary of State, the Legislature laid the foundation for the use of electronic signatures and electronic transactions in both state and local government.

5. Use of Electronic Signatures by Nongovernmental Entities

The ESAA also validated the use of electronic signatures between nongovernmental parties to a transaction.[88] However, this section went to great lengths to assure that there was agreement between the parties as to the use of electronic signatures before such a provision is applicable. This section also attempted to attain this assurance by focusing on the actions of the receiving party to determine whether such an agreement existed.

Section 6 stated that an electronic signature would be a valid signature in instances where it was authorized and accepted by the receiving party.[89] Under this section, the receiving party could determine the type of electronic signature that will be used in a transaction, provided that the receiving party gave notice to the signing party.

---

84 W. VA. CODE § 39-5-4(c), *repealed by* S.B. 204, enrolled April 14, 2001.

85 W. VA. CODE § 39-5-5(a), *repealed by* S.B. 204, enrolled April 14, 2001.

86 W. VA. CODE § 39-5-5(b), *repealed by* S.B. 204, enrolled April 14, 2001. It seems that the Governor's Office of Technology would also have the power to mandate certain technologies, such as digital signatures for use by state executive agencies. *See* W. VA. CODE § 5-1B-3 (1999).

87 W. VA. CODE § 39-5-7, *repealed by* S.B. 204, enrolled April 14, 2001.

88 W. VA. CODE § 39-5-6, *repealed by* S.B. 204, enrolled April 14, 2001.

89 W. VA. CODE § 39-5-6(a), *repealed by* S.B. 204, enrolled April 14, 2001.

6. Electronic Records

One of the purposes of the ESAA was to clarify the legal status of electronic records.[90] Section 2 defined a "record" as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form."[91] Although providing a definition, the ESAA failed to extend the same statutory weight to electronic records as it does to electronic signatures. Section 6 clearly validated electronic signatures under certain circumstances as they relate to messages between or among nongovernmental parties.[92] However, the ESAA omitted any direct verification of the legality of electronic records.[93]

The definition of "record" did serve to assure that the parties agree to the use of electronic signatures by requiring such "records" to be in a form that is retrievable by the receiving party.[94] Obviously, a receiving party is not going to agree to the substance of a record if it is sent in an indecipherable form.

7. Summary

The ESAA was the first step in recognizing the need to adapt West Virginia laws to the many dynamic changes in commercial transactions. The ESAA also opened the door for state and local governments to use electronic communications as a means to achieve greater efficiency. However, the ESAA was incomplete in many regards. It failed to provide protection for conforming parties against parties that failed to conform to agreed technological processes. It also did not provide any method for correcting errors or authorizing notarizations or authorizations. Further, the ESAA did not include provisions that would allow for the development and enforcement of electronic contracts or other agreements. The legislation also failed to establish standards by which an electronic record is deemed to have been sent or received.

West Virginia's adoption of the Uniform Electronic Transactions Act

---

90 W. VA. CODE § 39-5-1, *repealed by* S.B. 204, enrolled April 14, 2001.

91 W. VA. CODE § 39-5-2(f), *repealed by* S.B. 204, enrolled April 14, 2001.

92 W. VA. CODE § 39-5-6, *repealed by* S.B. 204, enrolled April 14, 2001.

93 In 1997, the Legislature created a records management and preservation board under section 5A-8-15 of the West Virginia Code, which was charged with the task of developing records management using electronic technology for county governments. *See* W. VA. CODE § 5A-8-15 (2000 & Supp. 2001). The legislation also permitted the board to extend its duties to a study of state agency record retention requirements. W. VA. CODE § 5A-8-15(h) (Supp. 2001). Final recommendations of the board for the use of electronic technology in county record management were due on July 1, 2001. W. VA. CODE § 5A-8-15(g) (Supp. 2001). A separate study is due April 1, 2002 for state agency document management standards. W. VA. CODE § 5A-8-15(h) (Supp. 2001). To date, although authorized, no members have been appointed by the Governor and no meetings have been conducted pursuant to this statute.

94 W. VA. CODE § 39-5-2(f), *repealed by* S.B. 204, enrolled April 14, 2001.

("WVUETA") addressed these and many other issues in a more comprehensive manner. The ESAA, however, did get the state "out of the box" and thinking about the adjustments that were needed to adapt our laws to the growth of electronic commerce.

C. *Financial Electronic Commerce Act*

In 1999, the Legislature promulgated another initiative intended to "facilitate and promote electronic commerce, particularly in the electronic receipting and disbursing of state funds."[95] Under this legislation, the State Auditor and State Treasurer were authorized to implement "electronic commerce . . . to facilitate the performance of their duties under the Code."[96] The bill also authorized the State Auditor to establish a state debit card known as the "West Virginia Check Card" for recipients of employee payroll, benefits, or entitlement programs that were not serviced by a federally insured deposit institution.[97] West Virginia Code section 12-3A-3 also contains a cryptic reference to authentication. It states "A record or an authentication used by the auditor or the treasurer may not be denied legal effect solely on the ground that it is in electronic form."[98] Although dealing with electronic authentication, no cross-reference is provided to ESAA or the WVUETA under sections 39-5-1 – 39-5-8 of the West Virginia Code. This left unanswered the standards under which electronic authentication and record keeping would be judged for the State Auditor's and State Treasurer's offices.

D. *The Medical Practices Act*

In 1999 the Legislature expanded the use of electronic signatures by permitting persons regulated under the Medical Practices Act "to utilize electronic signature or unique electronic identification to effectively sign materials, transmitted by computer or other means, upon which a signature is required for the purpose of authorized medical practice."[99]

Again, although statute authorizes the use of electronic signatures for regulated medical personnel, there is no cross-reference to the ESAA electronic signature guidelines of the WVUETA, leaving open the question of what standards will be used to judge electronic signatures for medical personnel. Moreover, there is no statutory guidance on what types of "unique electronic identification" other than electronic signatures would satisfy the requirements of sec-

---

95 W. VA. CODE § 12-3A-1 (2000).

96 W. VA. CODE § 12-3A-3 (2000).

97 W. VA. CODE § 12-3A-4 (2000).

98 W. VA. CODE § 12-3A-3 (2000).

99 W. VA. CODE § 30-3-13(d) (1998). The provision further provides that "[s]uch signatures are deemed legal and valid for purposes related to the provision of medical services." *Id.*

tion 30-3-13.[100]

These preliminary legislative actions, in conjunction with federal legislation regarding electronic commerce, set the stage for passage of a more comprehensive piece of legislation.

E. Uniform Electronic Transactions Act ("UETA")

Like West Virginia, many states have attempted to address the traditional contracts problem by enacting legislation that formally sanctions electronic contracts and signatures. For the most part, the legislation has been inconsistent from state to state. Although most statutes endorse electronic transactions, they vary in terms of determining the types of electronic technologies that will be acceptable.[101] A survey conducted by the Federal Reserve of Boston identified more than 2500 different state laws that require the issuer of checks to retain their cancelled checks.[102] This mass of rules and regulations effectively limits the ability of banks to automate the process.[103]

Moreover, the courts have been incongruous in applying traditional law to electronic transactions. Several courts have enforced electronic contracts if there was evidence of mutual assent between the parties.[104] On the other hand, courts have held that certain types of electronic agreements, such as tape-recorded contracts and facsimile notices, do not meet the writing requirements of the statute of frauds.[105]

In order to offer a source of stability, the National Conference of Commissioners on Uniform State Laws ("NCCUSL") developed the Uniform Electronic Transactions Act ("UETA") for adoption by the states. NCCUSL approved UETA at its annual meeting in July of 1999.[106]

---

[100] The failure to define the term "unique electronic identifier" leaves open the issue of what constitutes a valid electronic authentication. Under the ESAA, the use of a digitized signature would appear to satisfy this requirement for medical records – not a comforting thought. *See supra* note 39 and accompanying text.

[101] Scott Winkelman & Dylana Blum, *E-Commerce—Electronic Signatures Act*, NAT'L L.J., July 17, 2000, at B10.

[102] UNIF. ELECT. TRANSACTIONS ACT Prefatory Note, 7A U.L.A. 28, (Supp. 2001), *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (last visited Feb. 14, 2001) (on file with the *West Virginia Law Review*).

[103] UNIF. ELECT. TRANSACTIONS ACT, 7A U.L.A. 28 (Supp. 2001), *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (last visited Feb. 14, 2001) (on file with the *West Virginia Law Review*).

[104] *See, e.g.*, CompuServe, Inc. v. Patterson, 89 F.3d 1257, 1264 (6th Cir. 1996); Groff v. America Online, Inc., 1998 WL 307001, *5 (R.I. Super. Ct. May 27, 1998).

[105] Dep't of Transp. v. Norris, 474 S.E.2d 216, 218 (Ga. Ct. App. 1996) (facsimile transmission of notice of legal claim was not "written notice" according to Georgia law), *rev'd on other grounds*, 486 S.E.2d 826 (Ga. 1997); Roos v. Aloi, 487 N.Y.S.2d 637 (1985) (tape-recorded contract found unenforceable).

[106] *See* Patricia Brumfield Fry, *A Preliminary Analysis of Federal and State Electronic*

In promulgating the UETA, the NCCUSL sought to provide a national standard that would govern certain electronic transactions and bring a measure of consistency among the states.[107] Equally as important is the fact that UETA is not a law that attempts to alter substantive contract law.[108] Furthermore, the UETA is not a digital signature statute.[109] In cases in which states like West Virginia have adopted digital signature laws, the purpose of the UETA is to support and compliment such acts, not undermine them.[110]

Essentially, the UETA provides that:

a. A contract cannot be determined invalid simply because it is in an electronic form; and

b. An electronic signature shall be valid if it can be determined that it belongs to the apparent signer and that it represents the action of the signer.[111]

Because the UETA is a procedural statute, courts can still find electronic contracts unenforceable if they violate the state's substantive law (*e.g.*, a contract that is illegal or unconscionable or that is entered into under duress or fraud).

F. Electronic Signatures in Global and National Commerce Act ("E-SIGN")

"On June 30, 2000, President Clinton signed into law the Electronic Signatures in Global and National Commerce Act ("E-SIGN")."[112] The primary purpose of E-SIGN was to provide "a framework for the use and retention of electronic records and signatures."[113]

Commerce Laws, UETA Online, http://www.uetaonline.com/docs/pfry700.html (last visited June 19, 2001) (on file with *The West Virginia Law Review*).

[107] *Id.*

[108] *See* UNIF. ELECT. TRANSACTIONS ACT, 7A U.L.A. 28 (Supp. 2001), *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (last visited Feb. 14, 2001) (on file with the *West Virginia Law Review*). Because the UETA included provisions similar to the ESAA, West Virginia repealed the ESAA upon its adoption of the UETA.

[109] *Id.*

[110] *Id. See also* W. VA. CODE §§ 39-5-1 to -8 (Supp. 1998).

[111] UNIF. ELECT. TRANSACTIONS ACT, 7A U.L.A. 28 (Supp. 2001), *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (last visited Feb. 14, 2001) (on file with the *West Virginia Law Review*).

[112] Jim Whitter, *What Governors Need to Know About E-SIGN: The Federal Law Authorizing Electronic Signatures and Records*, http://www.nga.org/cda/files/000922ESIGN.PDF (last visited Feb. 14, 2001) (on file with *The West Virginia Law Review*).

[113] *Id.*

E-SIGN preempts state laws that only recognize records written on paper or manual signatures and those that invalidate contracts and signatures that appear in an electronic format.[114] However, section 7002(a) of E-SIGN provides that state law may modify, limit, or supersede the contracting provisions of E-SIGN if a state has enacted the UETA as approved by the NCCUSL in 1999.[115] Nevertheless, this preemption is subject to two stipulations.

First, if a state excludes further sections of state law under UETA section 3(b)(4), those sections are preempted to the extent they are inconsistent with Title I and Title II of E-SIGN.[116] These titles include the electronic contracting and transferable records provisions of E-SIGN.[117] In enacting Senate Bill 204, the West Virginia Legislature did not choose to exclude any additional state law provisions, as permitted under UETA section 3(b)(4).[118] Therefore, this section does not affect the ability of the West Virginia law to supersede the federal law.

Second, state law may modify, limit, or supersede the federal law only if it "specifies the alternative procedures or requirements for the use or acceptance . . . of electronic records or electronic signatures," provided:

a. the alternative procedures or requirements are consistent with Titles I and II; and

b. the alternative procedures do not require, or give greater legal status or effect to use or application of a specific technology or technological specification.[119]

West Virginia law mirrors the first sixteen required sections of the UETA to the extent that it supersedes federal law, as per E-SIGN section 7002(a).[120] Thus, further provisions that may be required under section 7002(a)(2) are not necessary so far as these sixteen provisions are concerned.[121]

---

[114] *Id.*

[115] Electronic Signatures in Global and National Commerce Act, 15 U.S.C.A. § 7002(a)(1) (Supp. 2001).

[116] Electronic Signatures in Global and National Commerce Act, 15 U.S.C.A. § 7002(a)(2)(A)(i) (Supp. 2001).

[117] Electronic Signatures in Global and National Commerce Act, 15 U.S.C.A. § 7002(a)(1) (Supp. 2001).

[118] *See generally* S.B. 204, 2001 Leg., 75th Sess. (W. Va. 2001).

[119] Electronic Signatures in Global and National Commerce Act, 15 U.S.C.A. § 7002(a)(2) (Supp. 2001).

[120] *See* W. VA. CODE § 39A-1-2 (Supp. 2001).

[121] Senate Bill 204 does include provisions regarding consumer protection that may be affected by section 102(a)(2) of E-SIGN. No analysis of this issue has been provided in this Article.

G. *Senate Bill 204*

On April 14, 2001, the West Virginia Legislature enacted Senate Bill 204. The provisions of Senate Bill 204 became effective July 13, 2001. Senate Bill 204 repealed the ESAA under Chapter 39, Article 5 of the West Virginia Code.[122] Essentially, however, Senate Bill 204 expanded the repealed provision.[123] The bill enacted a new Chapter 39A, Electronic Commerce, which contains three articles.

1. Article 1 – Uniform Electronic Transactions Act

West Virginia is one of thirty-nine states that have enacted the Uniform Electronic Transaction Act.[124] As of February 22, 2002, four other states are currently considering the UETA.[125] Article 1 embodies the UETA. The sections within Article 1 are virtually identical to the model language adopted by the NCCUSL.[126] However, there are some discrepancies that, upon examination, appear to be drafting errors.

Section 3, which pertains to the scope of the law, provides as follows:

> a. Except as otherwise provided in subsection (b), this [Act] applies to electronic records and electronic signatures relating to a transaction.
>
> b. This [Act] does not apply to a transaction to the extent it is governed by:
>
> (1) a law governing the creation and execution of wills, codicils, or testamentary trusts;
>
> (2) [The Uniform Commercial Code other than Sections 1-107 and 1-206, Article 2, and Article 2A];
>
> (3) [The Uniform Computer Information Transaction Act]; and

---

122 S.B. 204, 2001 Leg., 75th Sess. (W. Va. 2001).

123 *See supra* Part IV.D.

124 National Conference Commissioner on Uniform State Laws, *A Few Facts About . . . The Uniform Electronic Transactions Act*, http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp (last visited Feb. 22, 2002) (on file with the *West Virginia Law Review*).

125 *Id.*

126 UNIF. ELECT. TRANSACTIONS ACT, 7A U.L.A. 28 (Supp. 2001), *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (last visited Feb. 14, 2001) (on file with the *West Virginia Law Review*).

(4) [other laws, if any, identified by State].

c. This [Act] applies to an electronic record of electronic signature otherwise excluded from the application of this [Act] under subsection (b) to the extent it is governed by a law other than those specified in subsection (b).

d. A transaction subject to this [Act] is also subject to other applicable substantive law.[127]

The West Virginia Legislature did not include the invited provisions included in subsections (b)(3) and (b)(4).[128] Further, Senate Bill 204 naturally injects its own nomenclature regarding the identification of chapters, articles and sections.[129]

The first discrepancy is located in subsection (a). While the model provision states "except as otherwise provided in subsection (b)," the West Virginia provision states that "except as otherwise provided in subsection (d)."[130] In the context of the section, the West Virginia provision does not make sense and probably represents a drafting error.

In subsection (c), the West Virginia provision references other exclusions under subsection (b) "of this article."[131] Article 1 contains numerous subsections that are identified as"(b)." In the context of this section and the model code, the provisions should relate to subsection (b) "of this section," if it is necessary to mention the section at all. Under a literal reading of "under subsection (b) of this article," the confusion is compounded when this subsection further references "said subsection" at the close of the section.[132] If "said subsection" relates to "subsection (b) of this article," reference can be made to any subsection (b) in Article 1. This was clearly not the intent of the drafters, is inconsistent with the model act, and is almost certainly a drafting error.

2. Article 2 – Consumer Protection

Commentators were concerned that abandoning traditional paper writings could pose a danger to consumers in light of the protections that are af-

---

127 UNIF. ELECT. TRANSACTIONS ACT § 3, 7A U.L.A. 28 (Supp. 2001), *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (last visited Feb. 14, 2001) (on file with the *West Virginia Law Review*).

128 *See* W. VA. CODE § 39A-1-3 (Supp. 2001).

129 *See generally* S.B. 204, 2001 Leg., 75th Sess. (W. Va. 2001).

130 W. VA. CODE § 39A-1-3(a) (Supp. 2001).

131 W. VA. CODE § 39A-1-3(c) (Supp. 2001).

132 *Id.*

forded under various consumer protection laws.[133] In response to these concerns,[134] the West Virginia Legislature enacted Article 2, which attempts to provide the necessary protections.

In essence, Article 2 requires the consumer to consent to the use or retention of an electronic record and further requires that the consumer have access to an electronic record to which he or she is entitled.[135] The purpose of these provisions is to avoid unilateral actions that would place the consumer at a disadvantage.

3. Article 3 – Digital Signatures; State Electronic Records and Transactions

Article 3 is a recodification of several of the provisions contained in the ESAA, which has already been discussed.[136] These provisions are primarily concerned with the use of electronic records and electronic signatures in government transactions.[137]

West Virginia Code section 39A-3-1 adopts several of the definitions contained in former West Virginia Code section 39-5-2.[138] In particular, the new provision embraces the prior definitions of "certificate," "certification authority" and "digital mark."[139]

West Virginia Code section 39A-3-2 deals with the acceptance of electronic signatures by governmental entities in cases in which there is a signature requirement.[140] The provision is identical to former West Virginia Code section

---

133 *See* Shea C. Meehan, Comment, *Consumer Protection Law and the Uniform Electronic Transactions Act (UETA): Why States Should Adopt UETA as Drafted*, 36 IDAHO L. REV. 563, 563-64 (2000).

134 *See Uniform Electronic Transactions Act, Consumer Protections Needed: Hearing on S.B. 204 Before the S. Judiciary Subcomm. A*, 2000 Leg., 74th Sess. (W. Va. 2000) (statement of David P. McMahon).

135 W. VA. CODE §§ 39A-2-1 to -12 (Supp. 1998).

136 *See supra*, Part IV.B.

137 *See generally* W. VA. CODE §§ 39A-3-1 to -5 (Supp. 2001).

138 *See* W. VA. CODE § 39A-3-1 (Supp. 2001); W. VA. CODE § 39-5-2 (Supp. 1998).

139 W. VA. CODE § 39A-3-1 (Supp. 2001). Digital marks have been widespread in both consumer and governmental applications requiring interaction. This authentication device does not require an extensive infrastructure, as with digital signatures and certificates. The most common type of digital mark is the combination of a password and PIN number that restricts access to certain information, much like an ATM bank card. Institutions that control information can provide end-users with passwords and PIN numbers to access the information. The disadvantage of the digital mark is that authentication is tied to some prior communication between the parties. Hence, first-time users cannot reliably use a digital mark for authentication. The digital mark access method has been used in West Virginia for a variety of electronic information purposes including the ability to check on the status of NASCAR themed vanity license plate orders and income tax refunds.

140 W. VA. CODE § 39A-3-2 (Supp. 2001).

39-5-5 to the extent that subsection (a) references requirements and limitations contained in "section three of this article."[141] In the context of the new provision, this reference is inconsistent. Section 3 of this article pertains to the duties of the Secretary of State and the use of electronic signatures by state agencies.[142] Former section 39-5-3 set forth certain "requirements and limitations" that are now included in the UETA.

West Virginia Code section 39A-3-3 recodifies former section 39-5-4 of the ESAA.[143] Likewise, West Virginia Code section 39A-3-4 reinstates former section 39-5-7.[144] Senate Bill 204 did, however, add a severability clause, which the ESAA did not contain.[145]

4. More Consumer Protection

Senate Bill 204 also adds Article 6I to Chapter 46A, which provides further protection for consumers in situations involving electronic transactions.[146] In particular, the provision authorizes consumers to provide an electronic response to an electronic notice.[147] The article also sets forth the circumstances in which an electronic record has been statutorily received;[148] applies the provision to electronic transferable records;[149] and forbids parties to waive the provisions of the article.[150]

5. Relationship with E-SIGN

Section 5 specifically provides that the Legislature intended for this article to supplement, not modify, limit, or supersede E-SIGN.[151]

---

141 W. VA. CODE § 39-5-5, *repealed by* S.B. 204, enrolled April 14, 2001.

142 W. VA. CODE §§ 39A-3-1 to -5 (Supp. 2001).

143 W. VA. CODE § 39A-3-3 (Supp. 2001); W. VA. CODE § 39-5-4, *repealed by* S.B. 204, enrolled April 14, 2001.

144 W. VA. CODE § 39A-3-4 (Supp. 2001); W. VA. CODE § 39-5-7, *repealed by* S.B. 204, enrolled April 14, 2001.

145 W. VA. CODE § 39A-3-5 (Supp. 2001).

146 S.B. 204, 2001 Leg., 75th Sess. (W. Va. 2001).

147 W. VA. CODE § 46A-6I-2 (Supp. 2001).

148 W. VA. CODE § 46A-6I-3 (Supp. 2001).

149 W. VA. CODE § 46A-6I-4 (Supp. 2001).

150 W. VA. CODE § 46A-6I-6 (Supp. 2001).

151 W. VA. CODE § 46A-6I-5 (Supp. 2001).

V. WEST VIRGINIA'S UNIFORM ELECTRONIC TRANSACTIONS ACT ("WVUETA")

A. *Purpose of the WVUETA*

The primary purpose of the WVUETA is to assure parties who engage in electronic commerce that their transactions are as enforceable as those that are conducted through traditional methods (such as handwritten signatures) without altering any of the substantive rules that apply to the transaction.[152] Although there are numerous issues that have evolved with the growth of electronic commerce, this purpose is quite narrow – guaranteeing that an electronic record is the equivalent of a paper record and that an electronic signature has the same effect as a handwritten signature.[153]

The foundation for achieving this limited objective is contained in West Virginia Code section 39A-1-7, which states that a record or signature will not be denied electronic effect or enforceability solely because it is in an electronic form.[154] This provision is designed to eliminate any notion that signatures or records must be in the form of paper and pen in order to be legally enforceable.[155]

The definition of an electronic signature includes "an electric sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."[156] Thus, an electronic signature must meet three criteria. The first is the rather broad requirement that the electronic signature consist of an electric sound, symbol, or process.[157] This section does not require the use of a specific technology.[158] A recorded voice may suffice if the other two qualifications are met.[159]

Second, the electronic sound, symbol or process must be "attached to or logically associated" with the record.[160] In traditional transactions, the signature on the page or symbol attached thereto is a part of some manifestation of the transaction. Such a tangible display is not present in an electronic transaction,

---

152 W. VA. CODE § 39A-1-7(a) (Supp. 2001).

153 *Id.*

154 W. VA. CODE §§ 39A-1-7(a)–(b) (Supp. 2001).

155 W. VA. CODE §§ 39A-1-7(c)–(d) (Supp. 2001).

156 W. VA. CODE § 39A-1-2(7) (Supp. 2001). The WVUETA definition of "electronic signature" is similar to the ESAA definition except that the new definition replaces the descriptive phrase "identifier or authentication technique" with "electronic sound, symbol or process." W. VA. CODE § 39-5-2(e) (Supp. 1998).

157 W. VA. CODE § 39A-1-2(8) (Supp. 2001).

158 *See id.*

159 W. VA. CODE § 39A-1-2(13) (Supp. 2001).

160 W. VA. CODE § 39A-1-2(8) (Supp. 2001).

prompting the need for a subjective determination as to the relationship between the symbol or sign and the electronic document.[161]

Third, the critical prerequisite is that the party intended to sign the document.[162] Once again, the party's intention would depend upon the facts and circumstances surrounding the transaction.[163]

An electronic record is broadly defined as "a record created, generated, sent, communicated, received, or stored by electronic means."[164] In other words, an electronic record is any type of record created, used, or stored by some means other than paper.

Although subsections (a) and (b) are prohibitive in nature, subsections (c) and (d) positively declare that the requirement that a record or signature be in writing will be satisfied if the record or signature is in an electronic format.[165] This provision validates electronic records and signatures subject to the other provisions of the article.[166]

B. Scope of the WVUETA

The WVUETA pertains to the means in which records or signatures can meet the terms of the law. Under the WVUETA, records or signatures that appear in electronic format will be deemed to be legally sufficient.[167] However, the types of activities in which electronic records or signatures shall be accepted are limited.[168]

Section 3 limits the application of the WVUETA to "electronic records and electronic signatures relating to a transaction."[169] The WVUETA defines

---

161 In application, the digital signature is typically transmitted as part of the original message or is electronically linked to that message.

162 W. VA. CODE § 39A-1-2(8) (Supp. 2001).

163 UNIF. ELECT. TRANSACTIONS ACT, 7A U.L.A. 28 (Supp. 2001), *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (last visited Feb. 14, 2001) (on file with the *West Virginia Law Review*). Again, the application of a digital signature to a document requires the user to proactively access the program that produces the signature. This act is equated with the affirmative action of intending to sign a document. *Id.*

164 W. VA. CODE § 39A-1-2(7) (Supp. 2001). The WVUETA definition of "electronic record" is similar to the ESAA definition, but the new provision expands the term to include records that are "created" or "sent." W. VA. CODE § 39-5-2(d) (Supp. 1998). Subsection (13) of this section defines a "record" as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." W. VA. CODE § 39A-1-2(13) (Supp. 2001).

165 W. VA. CODE § 39A-1-7 (Supp. 2001).

166 *Id.*

167 W. VA. CODE § 39A-1-2 (Supp. 2001).

168 W. VA. CODE § 39A-1-3 (Supp. 2001).

169 *Id.*

"transaction" as "an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs."[170] Thus, the WVUETA does not apply to all writings and signatures, but is confined to those electronic records or signatures that relate to interactions between parties involved in a business, commercial, or governmental activity.[171]

Moreover, section 3 further excludes certain types of transactions that may otherwise be included in the definition of "transaction."[172] The WVUETA does not apply to wills, codicils, or testamentary trusts.[173] The WVUETA also does not apply to the Uniform Commercial Code except for provisions that deal with the sale or lease of personal property.[174]

In some instances, more than one law may cover a transaction that involves an electronic record or signature. In those cases, the WVUETA will apply to an electronic record or electronic signature that may be excluded under section 3 to the extent that it is covered by another law.[175] For example, the WVUETA does not validate electronic checks because checks are governed by Article 4 of the UCC, which is excluded by section 3. However, the same elec-

---

[170] W. VA. CODE § 39A-1-1(16) (Supp. 2001).

[171] "Commercial" activity includes consumer affairs. *See* UNIF. ELECT. TRANSACTIONS ACT § 3, cmt. 1, 7A U.L.A. 28 (Supp. 2001), *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (last visited Feb. 14, 2001) (on file with the *West Virginia Law Review*).

[172] W. VA. CODE § 39A-1-3 (Supp. 2001).

[173] W. VA. CODE § 39A-1-3(b)(1) (Supp. 2001).

West Virginia Code section 41-1-3, pertaining to wills and codicils, provides as follows:

> No will shall be valid *unless it be in writing* and *signed by the testator*, or by some other person in his presence and by his direction, in such manner as to make it manifest that the name is intended as a signature; and moreover, unless it be *wholly in the handwriting of the testator*, the signature shall be made or the will acknowledged by him in the presence of at least two competent witnesses, present at the same time; and such witnesses shall subscribe the will in the presence of the testator, and of each other, but no form of attestation shall be necessary.

W. VA. CODE § 41-1-3 (1997) (emphasis added). Interestingly, the "handwriting" requirements set forth in section 41-1-3 are not addressed in the Act. *See generally* W. VA. CODE §§ 39A-1-1 to -3-5 (Supp. 2001). This leaves open the question whether a document with a proper digital signature satisfies the "handwriting" requirements in various Code sections. *See, e.g.*, W. VA. CODE § 8-8-2 (1997) (requiring that voter petitions to municipalities be "signed in their own handwriting" by twenty percent or more of qualified voters). If these voters submitted an electronic petition containing valid digital signatures would that voter petition be valid?

[174] W. VA. CODE § 39A-1-3(b)(2) (Supp. 2001). WVUETA applies to Chapter 46, Articles 1 and 2, which pertain to the sale and lease of goods respectively. WVUETA, by exception, also applies to West Virginia Code section 46-1-107 (regarding the waiver or renunciation of a claim or right after a breach) and West Virginia Code section 46-1-206 (regarding the statute of frauds). W. VA. CODE § 39A-1-3(2) (Supp. 2001).

[175] W. VA. CODE § 39A-1-3(c) (Supp. 2001).

tronic record of a check may be governed by the section of the WVUETA that applies to the retention of an electronic image or record of a check.[176]

C. *Application of the WVUETA*

1. Liberal Interpretation

Today we are witnessing advancements in technology that were totally unforeseen just a decade ago. Consequently, we can anticipate with reasonable certainty that things will continue to change. The WVUETA recognizes the high probability of change by setting forth several broad guidelines for use in future interpretations of the Act.

First, section 6 requires the WVUETA to be interpreted in a manner that will "facilitate electronic transactions consistent with other applicable law."[177] Second, any interpretation of the WVUETA must be "consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices."[178] Third, the WVUETA must be used to "effectuate its general purpose to make uniform the law with respect to the subject of this article among states enacting it."[179]

In short, the provisions of section 6 provide for the utmost flexibility in applying the WVUETA for the purposes of validating electronic records and electronic signatures.

2. Agreement Between Parties

The WVUETA cannot require persons engaged in a particular transaction to use an electronic record or electronic signature.[180] The parties to such transaction must agree. Once agreed, however, a sender will satisfy a law that requires him to deliver information to another person when he provides, sends or delivers the information in such a form that the recipient will be able read and retain the electronic record for future use.[181] A sender will not satisfy the law if he employs a technology that hinders the ability of the recipient to retain and review the information.[182] Thus, the sender has the burden of insuring that the

---

176 West Virginia Code section 39A-1-12 relates to electronic records. *See* UNIF. ELECT. TRANSACTIONS ACT § 3, cmt. 8, 7A U.L.A. 28 (Supp. 2001), *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (last visited Feb. 14, 2001) (on file with the *West Virginia Law Review*).

177 W. VA. CODE § 39A-1-6(1) (Supp. 2001).

178 W. VA. CODE § 39A-1-6(2) (Supp. 2001).

179 W. VA. CODE § 39A-1-6(3) (Supp. 2001).

180 W. VA. CODE § 39A-1-5(a) (Supp. 2001).

181 W. VA. CODE § 39A-1-8(a) (Supp. 2001).

182 W. VA. CODE § 39A-1-8(c) (Supp. 2001).

recipient is capable of receiving the information. In some instances, recipients may use a peculiar type of technology to avoid the receipt of such information. Despite the burden that the WVUETA clearly places upon the sender, courts would probably view the sender as compliant if the recipient engages in such shenanigans.

3. Specified Manner of Transmission

The WVUETA may not override laws that require records to be posted or displayed in a specific manner; sent, communicated, or transmitted by a specific method; or formatted in a certain manner. Senders and recipients may not rely upon the WVUETA to circumvent those provisions.[183] This would include attempts by senders and recipients to rely upon an agreement to use a nonspecific manner except in cases in which:

a. The law clearly permits variation by agreement; and

b. Other provisions of the law permits parties required to use first class mail, postage prepaid, regular U.S. mail, certified mail or registered mail to use another method.[184]

4. Attribution of Electronic Signatures and Records

In transactions between parties, it is important that the record that results or the signature that a party uses to confirm an action is attributable to the respective party. The WVUETA attributes an electronic record or electronic signature to a particular person if it can be determined in any manner that the record or signature was the act of such person.[185] For example, both an electronic record and electronic signature would be attributable to a person in instances in which either a person or the person's agent types the person's name as part of an e-mail-based purchase order. Another similar situation is one in which a person's computer issues a purchase order that contains identifying information pursuant to a program that orders goods upon receipt of certain information.[186] Once an electronic record or electronic signature is attributed to a particular person, the facts and circumstances surrounding the transaction determine the effect.[187]

---

183 W. VA. CODE § 39A-1-8(b) (Supp. 2001).

184 W. VA. CODE § 39A-1-8(d) (Supp. 2001).

185 W. VA. CODE § 39A-1-9(a) (Supp. 2001).

186 UNIF. ELECT. TRANSACTIONS ACT § 9, cmt. 1, 7A U.L.A. 28 (Supp. 2001), *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (last visited Feb. 14, 2001) (on file with the *West Virginia Law Review*).

187 W. VA. CODE § 39A-1-9(b) (Supp. 2001).

5. Effect of Change or Error in Transmission

The WVUETA specifically addresses circumstances in which changes or errors occur during the transmission of a record.[188] As an example of the difference between the two, assume that an automobile repair shop electronically orders one carburetor for a 1962 Nash Rambler from a parts dealer. In processing the order, the dealer's computer alters the order and sends out ten carburetors to the repair shop. In this case, a "change" has occurred. Conversely, if a mechanic at the repair shop had mistakenly typed in "10" carburetors instead of "1" and transmitted the order to the dealer, an "error" would have occurred.

The WVUETA provides statutory guidance in two types of cases. The first case involves an occasion in which (1) the parties are utilizing an agreed-upon security procedure to detect "changes" or "errors" and (2) one party has conformed to the procedure and the other has not. In such an instance, the conforming party can avoid the effect of the change or error if the nonconforming party would have detected the change or error had he followed the security procedures.[189]

The WVUETA also applies in cases in which individuals wish to avoid the effect of a mistake occurring during the course of an automated transaction with the electronic agent of the other party. The WVUETA defines an "automated transaction" as

> a transaction conducted or performed, in whole or in part, by electronic means or electronic records in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract or fulfilling an obligation required by the transaction.[190]

Under this definition, the important factor in determining the existence of an "automated transaction" is in circumstances in which human review by either party is not anticipated. A familiar such transaction may involve ordering a book from Amazon.com, where an order is confirmed and processed by the book company's computer. In this case, the computer (or, more specifically, the computer's program) acts as an "electronic agent" for Amazon.com.[191] In such a

---

188 Note that the WVUETA only addresses changes or errors in transmission and not changes or errors that may occur otherwise. In such cases, the law of mistake provides the basis for addressing any conflict.

189 W. VA. CODE § 39A-1-10(1) (Supp. 2001).

190 W. VA. CODE § 39A-1-2(2) (Supp. 2001).

191 West Virginia Code section 39A-1-(6) defines "electronic agent" as "a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances, in whole or in part, without review or action by an individual." W. VA. CODE § 39A-1-(6) (Supp. 2001).

situation, the mistaken party may avoid the potential adverse effects of the error if:

a. the computer program failed to provide the mistaken party with an opportunity to prevent or correct the error;

b. the mistaken party promptly notifies the other party of the error and indicated that he did not intend to be bound by the electronic record;

c. the mistaken party takes reasonable steps to conform to the other person's reasonable instructions;[192] and

d. the mistaken party has not received any benefit or value from the consideration received from the other person.[193]

In circumstances in which neither factual situation is present, the parties must rely upon the traditional law of mistake, the contract between the parties, or some other form of law.[194] Only in cases involving agreed-upon security procedures may parties to a transaction agree to avoid this section of the WVUETA.[195]

6. Notaries and Acknowledgements

One of the most common and traditional means of validating a writing is through the use of a notarization, acknowledgement, or verification made under oath. Under the WVUETA, an electronic signature may be used if the electronic signature of the person authorized to make an affirmation is "attached to or logically associated with the signature or record."[196]

D. Electronic Records

1. Retention

Under the WVUETA, an electronic record is legally sufficient if it accurately reflects the information "as it was first generated" and the information is accessible at a later date.[197] This applies even in situations in which the law re-

---

[192] These instructions may include returning the consideration to the other person or destroying the consideration.

[193] W. VA. CODE § 39A-1-10(2) (Supp. 2001).

[194] W. VA. CODE § 39A-1-10(3) (Supp. 2001).

[195] W. VA. CODE § 39A-1-10(4) (Supp. 2001).

[196] W. VA. CODE § 39A-1-11 (Supp. 2001).

[197] W. VA. CODE § 39A-1-12(a) (Supp. 2001).

quires a record to be *presented or retained* in its original form.[198] In particular, the WVUETA states that check retention laws shall be satisfied if the information contained on the front and back of the check are retained in electronic form.[199]

In general, records kept for evidentiary, auditing, or other similar purposes will satisfy state law if they are retained in electronic form.[200] This includes evidence that may be offered in a proceeding.[201] However, the State retains the right to require that government records be retained in a specified form.[202]

2. Transferable Records

a. In General

The WVUETA amends the UCC to authorize the use of "transferable records" in an electronic format. The WVUETA limits this use to the creation, transferability, and enforceability of promissory notes and documents of title in cases in which the issuer has agreed to use an electronic medium.[203] Thus, checks and other systems of payment governed by Articles 3 and 4 of the Uniform Commercial Code are not included.

b. Ownership and Control

In the paper world, possession is a necessary element in determining the ownership of a promissory note or document of title. Obviously, in the digital

---

198 W. VA. CODE § 39A-1-12(d) (Supp. 2001). Contrast this provision with West Virginia Code section 39A-1-8(b), which provides that the WVUETA may *not* override laws that require records "to be posted or displayed in a specific manner," "to be sent, communicated or transmitted by a specified method," or "to contain information that is formatted in a certain manner." W. Va. Code § 39A-1-8 (Supp. 2001). Thus, it appears that records may be converted to an electronic format for retention and future evidentiary purposes, but may only be communicated in some fashion in its original form if statutorily required.

199 W. VA. CODE § 39A-1-12(e) (Supp. 2001). The WVUETA specifically singles out check retention in response to a survey conducted by the Federal Reserve Bank of Boston, which found hundreds of state laws that required checks to be retained in their original form. The National Conference of Commissioners on Uniform State Laws believed that such laws precluded banks and their customers from enjoying the convenience and efficiencies created by electronic retention. UNIF. ELECT. TRANSACTIONS ACT § 12, cmt. 6, 7A U.L.A. 28 (Supp. 2001), *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (last visited Feb. 14, 2001) (on file with the *West Virginia Law Review*).

200 W. VA. CODE § 39A-1-12(f) (Supp. 2001).

201 W. VA. CODE § 39A-1-13 (Supp. 2001).

202 W. VA. CODE § 39A-1-12(g) (Supp. 2001).

203 West Virginia Code section 39A-1-16(a) specifically references Chapter 46, Articles 3 and 7.

world, it would be quite difficult to determine possession in the same sense. Under the WVUETA, "control" is a substitute for possession as well as for the requirements of delivery and indorsement.

West Virginia Code section 39A-1-16(b) states that "[a] person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred."[204]

To satisfy this provision, a system must satisfy a list of strict requirements. First, the system must be able to create, store, and assign a single authoritative copy of the transferable record that is unique, identifiable, and unalterable.[205] Second, the authoritative copy must identify the person who asserts control as the person to whom the transferable record was issued or, if previously transferred, the person to whom the transferable record was most recently transferred.[206] Finally, the authoritative copy must be communicated to and maintained by the person asserting control or his designated custodian.[207] Reference to a designated custodian indicates permission to use a trusted third party that, likewise, meets these requirements.

By requiring these safeguards, the WVUETA is mindful of the need to establish a system that will provide legal certainty as to the "holder" of a promissory note or document of title and the ability to maintain the identity of successive holders upon transfer.

c. Rights and Defenses

Once control is determined, the person exercising control becomes the holder of the promissory note or document of title. The WVUETA establishes the rights and defenses of holders of transferable records by referencing the sections of Articles 3, 7 and 9 of Chapter 46 that relate to the rights and defenses of a holder in due course, a holder of a negotiable title or a purchaser.[208]

Likewise, an obligor would have the same rights and defenses that exist had he used a traditional paper method.[209] In addition, the WVUETA grants the obligor the right to access the transferable record and other information in order

---

[204] W. VA. CODE § 39A-1-16(b) (Supp. 2001).

[205] A "transferable record" can be copied or revised in cases in which the person in control consents, the copy is identified as such, and any revision is readily identifiable. W. VA. CODE § 39A-1-16(c)(4)–(6) (Supp. 2001). "Unalterable," as used in this context, would seem to require that any record be stored electronically in a "read only" format, or such record would need to be written to unalterable electronic media, such as optical or read-only compact disc.

[206] W. VA. CODE § 39A-1-16(c) (Supp. 2001).

[207] W. VA. CODE § 39A-1-16(c)(1)–(3) (Supp. 2001).

[208] W. VA. CODE § 39A-1-16(d) (Supp. 2001).

[209] W. VA. CODE § 39A-1-16(e) (Supp. 2001).

that he may be certain who is to pay.[210]

E. Other Provisions

1. Automated Transaction Rules

An integral part of any electronic transaction is the machines that do the work. In essence, computers and computer programs serve as agents for the contracting parties. The WVUETA sanctions the use of computers and their programs as electronic agents for parties to a contract even in circumstances in which there is no review by an individual.[211] Thus, ordering a book through the Amazon.com computer system binds the company to sell the purchaser a book despite the fact that no employee reviewed or approved of the sale.[212]

2. Time and Place of Sending and Delivery

Unless agreed otherwise, an electronic record is sent and received when the system that is designated by the recipient receives the record or information in a form that it can process and the record becomes under the control of the recipient.[213] Moreover, the WVUETA deems an electronic record to be sent from the sender's place of business to the recipient's place of business even if the location of the recipient's information processing system is different from the deemed location.[214]

Mere receipt, however, does not prove that the content sent was the same as the content received.[215] When a person purports that the content is different, other applicable law determines the legal effect of the sending and receiving.[216]

---

210 W. VA. CODE § 39A-1-16(f) (Supp. 2001).

211 W. VA. CODE § 39A-1-14(a) (Supp. 2001).

212 However, the terms of the contract would be subject to substantive rules of law. W. VA. CODE § 39A-1-14(3) (Supp. 2001).

213 W. VA. CODE § 39A-1-15(a)–(b) (Supp. 2001). Under section 15(e), an electronic record is received even if no individual is aware of the receipt. W. VA. CODE § 39A-1-15(e) (Supp. 2001). Nevertheless, receipt of acknowledgement from an information processing system, as described in subsection (b), does not, by itself, establish that the content sent corresponds to the content received. W. VA. CODE § 39A-1-15(f) (Supp. 2001).

214 W. VA. CODE § 39A-1-15(c)–(d) (Supp. 2001). The WVUETA provides several guidelines for particular instances. For example, if the sender or recipient has more than one place of business, the place of business shall be the location having the "closest relationship to the underlying transaction." If the sender or recipient does not have a place of business, his or her residence will be used. W. VA. CODE § 39A-1-15(d)(2) (Supp. 2001).

215 W. VA. CODE § 39A-1-16(f) (Supp. 2001).

216 W. VA. CODE § 39A-1-16(g) (Supp. 2001).

3. Relationship with E-SIGN

In order to avoid potential preemption, the West Virginia Legislature included a special section that specifically provides that the enactment of Chapter 39A, Article 1 is the enactment of the WVUETA.[217]

4. Choice of Law for Computer Information Agreements

In a move that is intended to blunt the "choice of forum" laws contained in the Uniform Computer Information Transaction Act ("UCITA"), the WVUETA adds section 55-8-15, which provides that residents of West Virginia may choose to void any provision that attempts to interpret contracts according to the laws of states that have adopted the UCITA[218] or "substantially similar"[219] provisions.[220]

This provision, which has been adopted in other states, is a reaction to the perceived "pro-company" slant of the UCITA. Under the model act, software licenses are to be interpreted under the state law where the software company is resident. For example, a company doing business in Virginia and selling consumer software products in West Virginia under a "computer information agreement" can specify that the software license be interpreted *under Virginia law* and *adjudicated in Virginia*. This creates clear inequities in the case of consumer product sales. Under section 55-8-15, a West Virginia resident (or an organization with its principal place of business in West Virginia) can choose to void the choice of forum provision in the software license and adjudicate the action in West Virginia.[221]

VI. CONSTRUCTING THE DIGITAL CERTIFICATE INFRASTRUCTURE

A. *Powers of the Secretary of State*

Section 39A-3-3(a) of the West Virginia Code provides that the Secretary of State is to issue legislative rules to facilitate the use of electronic signatures in government transactions.[222] Section 39A-3-3(b) designates the Secretary

---

217 W. VA. CODE § 39A-1-17 (Supp. 2001).

218 To date, only Maryland and Virginia have adopted the model UCITA legislation.

219 W. VA. CODE § 55-8-15 (1997).

220 *See* Ed Foster, *What Widespread Enactment of UCITA Could Mean*, InfoWorld, http://www.infoworld.com/articles/uc/xml/00/08/21/000821ucissues.xml (Aug. 18, 2000) (pro-consumer overview of UCITA provisions) (on file with *The West Virginia Law Review*).

221 W. Va. Code § 55-8-15 (2000)

222 Pursuant to West Virginia Code section 64-9-2, these legislative regulations will apparently supercede those that were issued under repealed sections 39-5-1 to -5-8. *See also supra* note 48 and accompanying text.

of State as the certification authority and repository for all government agencies subject to chapter 29A of the Code.[223] In addition, the Secretary of State "may propose legislative rules for issuing certificates that bind public keys to individuals, and other electronic transaction authentication devices as provided for in this article."[224] This would seem to permit the Secretary of State to issue regulations that extend to individual use of PKI digital signatures and certificates within the state. The provision also allows the Secretary of State to contract with private parties to accomplish these tasks.[225]

Section 39A-3-4 of the Code permits the Secretary of State to revoke any digital certificate if there is reason to believe that it has been stolen or fraudulently obtained.[226] This section also insulates the Secretary of State from any liability arising out of the illegal or improper use of electronic signatures.[227]

B. Business and Audit Guidelines for Digital Certificates

In promulgating rules to implement a digital certificate infrastructure, care must be taken in creating a system that complies with appropriate business and auditing practices.[228] The American Bar Association recently released a draft assessment document that is intended to act as a guide in implementing PKI systems.[229] This document provides guidance on the use of PKI, and an introduction to PKI assessment models. More importantly, it provides guidance on the selection of policies, standards, and legal agreements between certification authorities, subscribers (*i.e.*, private key holders using the certification authorities), relying parties (organizations relying on use of the public key to validate transactions), registration authorities (organizations assisting a certification authority in authenticating the identity of an individual or business) and repositories (those organizations that provide storage, publication and access to certificates).[230] Many of the guidelines outlined in this draft assessment have already been implemented by state certification authorities.[231]

---

223 W. VA. CODE § 39A-3-3(b) (Supp. 2001).

224 *Id.*

225 Private firms such as Verisign and Thawte provide outsourcing for the issuance of digital signatures and certificates.

226 W. VA. CODE § 39A-3-4 (Supp. 2000).

227 *Id.*

228 The American Institute of Certified Public Accountants, *WebTrust Program for Certification Authorities, v. 1.*, *available at* http://ftp.webtrust.org/webtrust_public/certauth_fin.doc (Aug. 25, 2000) (on file with *The West Virginia Law Review*).

229 *See* PAG, *supra* note 25, at 14.

230 *See id.* at 26.

231 *See, e.g.*, Washington Authentication Administrative Rules, WASH. ADMIN. CODE §§ 434-180-200, -240, -360, *available at* http://search.leg.wa.gov/wslwac/WAC%20434%20%20TITLE/WAC%20434%20-

VI. CONCLUSION – WHAT NEXT?

West Virginia has embraced the information economy as a means of bridging the gap between the "old" economy and the "new." The digital age has already benefited the West Virginia economic landscape in the form of E-Commerce activities[232] and the recent statutory developments are promising to improve the digital delivery, authentication, and storage of electronic documents within the state. Although the recent statutory developments outlined above have pushed West Virginia forward, there is still much that needs to be accomplished.

First, the digital certificate infrastructure that is outlined in the WVUETA must be implemented by private firms and governmental agencies within the state. Although "workarounds" are available to allow valid electronic transactions, in the long run, the digital signature/certificate authority provides the most efficient means of conducting electronic commerce and opening up of government to citizen access.

The allure of the information age lies in the ability to deliver, store, and access information in digital form. In that regard, the Legislature must revisit statutory frameworks and review those guidelines in light of the goal of leveraging the power of technology. We have noted several instances in which statutes need to be revised or, at a minimum, cross-referenced with technology-specific items. Specifically, we need to push forward at both the statutory and regulatory levels for guidance in the use of information technology in record capture and retention, information reporting, and government/citizen interaction (including voting), if we are to move further into the information age.

Certainly the rapid change endemic to the "information age" has created pressures on the law to keep pace. The actions by the West Virginia Legislature over the past several years have created a flexible statutory framework for future action.

180%20%20CHAPTER/WAC%20434%20-180%20%20CHAPTER.htm (last updated Oct. 25, 2000).

[232] For example, Amazon.com opened a call center and warehouse in Huntington, West Virginia in 1999. Coldwater Creek operates a similar facility in Parkersburg, West Virginia.